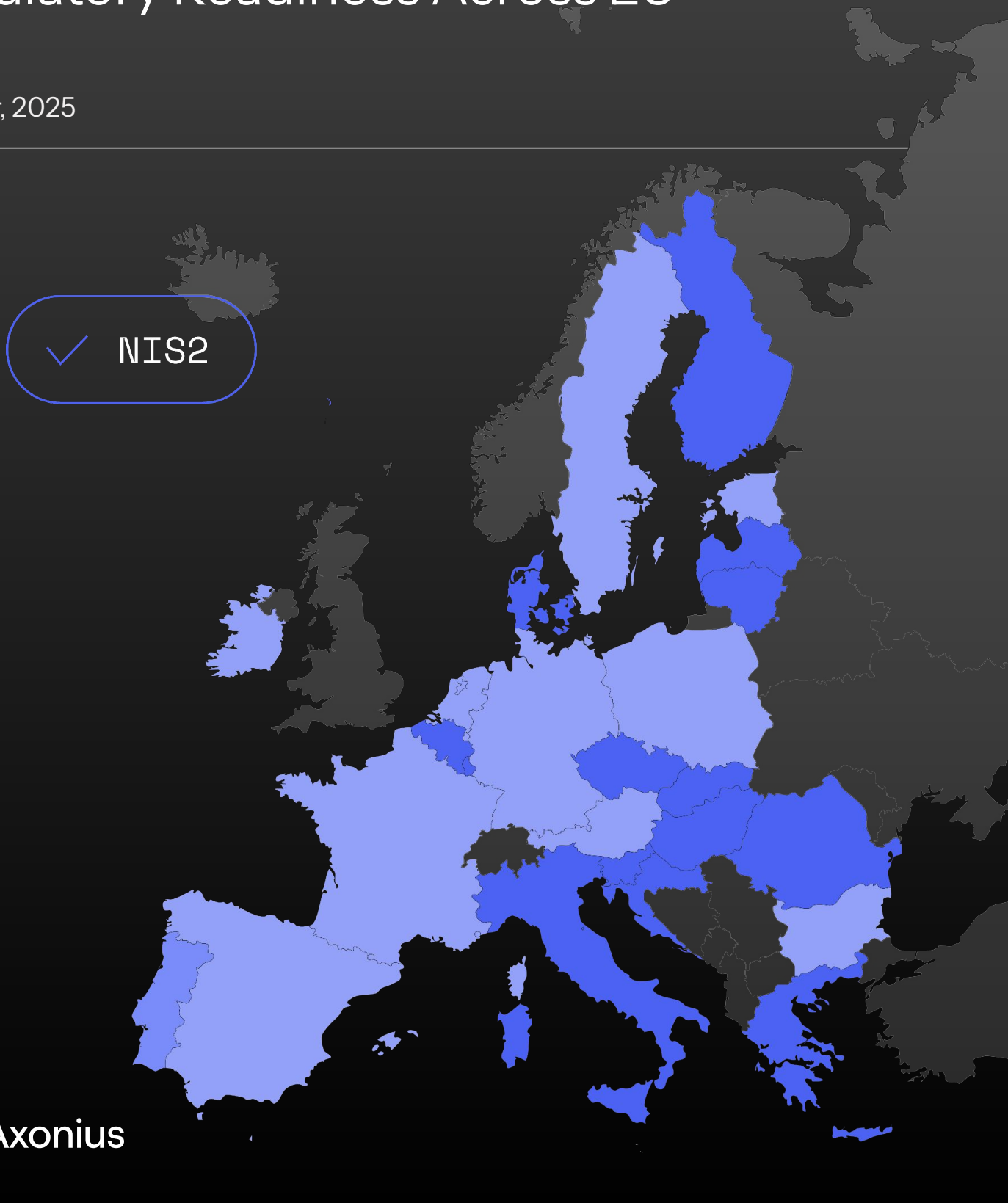
EBOOK

Axonius for NIS2 Compliance

Achieving Cyber Resilience and Regulatory Readiness Across EU

October, 2025



Axonius

Table of Contents

Executive Summary

Disclaimer

This document is provided for informational purposes only and does not constitute legal, regulatory, or compliance advice. Organizations should consult their legal, regulatory, or cybersecurity advisors to determine how the NIS2 Directive and related national laws apply to their specific circumstances.

The EU's ***Network and Information Systems Directive 2 (NIS2)*** is the bedrock of the European Union's new cybersecurity framework, requiring all essential and important entities to implement structured, risk-based security measures and report incidents to national authorities. It elevates cybersecurity to a matter of executive responsibility, combining continuous risk management, incident readiness, supply chain assurance, and threat intelligence sharing with strict accountability and significant penalties for non-compliance.

With national transpositions now taking effect across the EU, albeit with some delays typical of large-scale EU regulatory rollouts, organizations must demonstrate real-time visibility, control, and governance over their digital environments.

Many entities still struggle with fragmented asset inventories, incomplete risk mapping, and manual evidence collection, making compliance slow and costly. Axonius addresses these challenges through Cyber Asset Attack Surface Management (CAASM), unifying data from over 1,200 integrations to create a single source of truth for assets, identities, and vulnerabilities.

By automating discovery, correlation, and compliance reporting, Axonius helps organizations meet NIS2 Article 21 requirements for risk management and Article 23 obligations for incident reporting. Customers achieve faster audit readiness, up to 75% time savings, as reported in The Total Economic Impact™ of Axonius study by Forrester Consulting (2023) in compliance preparation, and stronger resilience against supply-chain and insider threats. NIS2, if seen with the right lens, can transform a regulatory burden into an operational advantage.

This eBook offers comprehensive guidance towards NIS2 compliance, addressing the new realities for essential and important entities. It presents a practical operating model for continuous compliance through a control loop. The eBook details how Axonius aligns with Articles 21, 23, and 24 of NIS2 and illustrates how the platform supports compliance by showing how data flow, policy enforcement, and automation layers work together to deliver measurable outcomes.

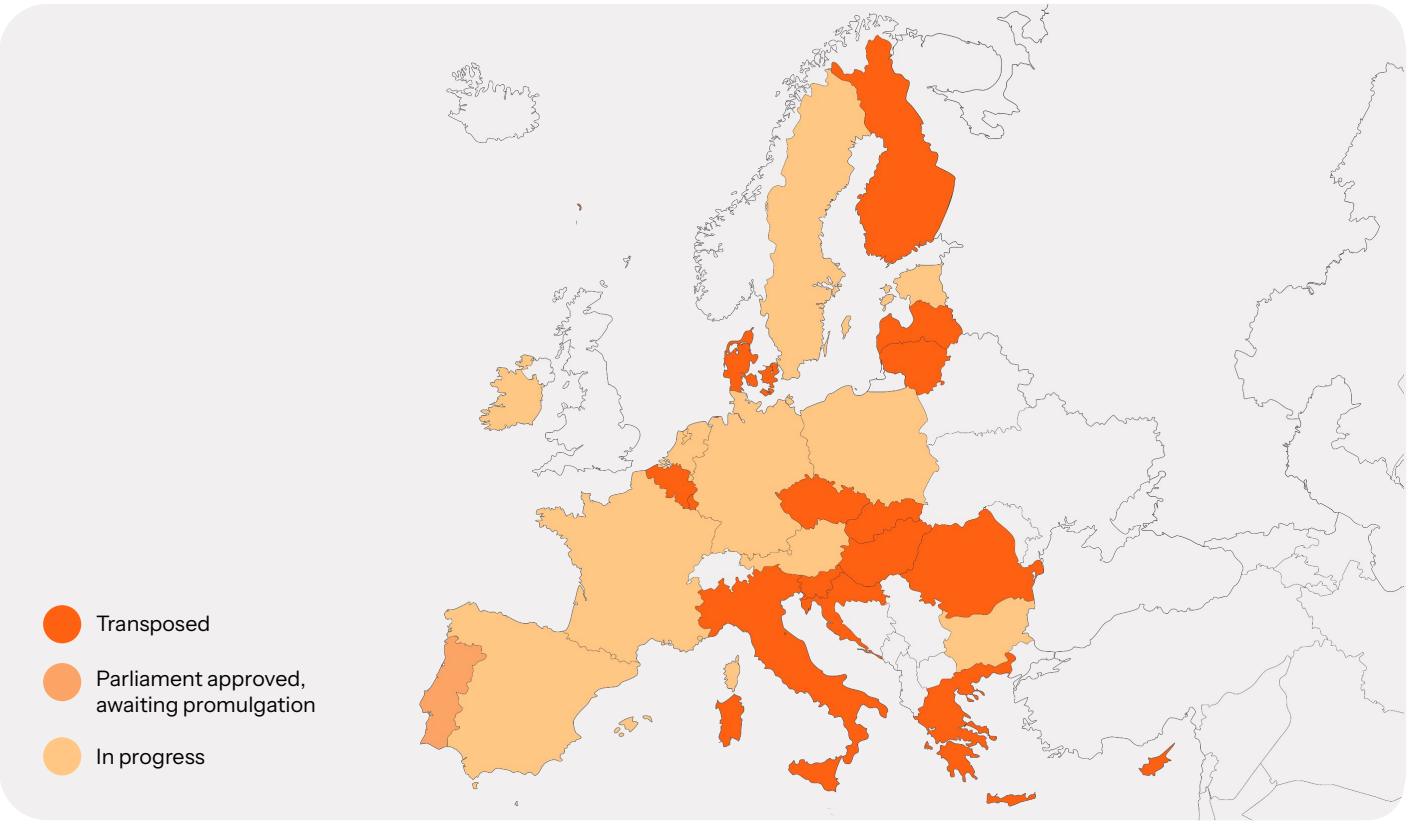
The NIS2 Context in EU

The Regulatory Landscape

The rationale behind Network and Information Systems Directive 2 (NIS2) is to create a harmonized framework for cybersecurity risk management and incident reporting across the EU to safeguard its economy, critical infrastructure, and overall resilience. By expanding both scope and accountability, NIS2 replaces the 2016 directive and now covers a larger number of business sectors such as utilities, finance, healthcare, digital infrastructure, and public administration. Its purpose is to strengthen resilience and ensure that both essential and important entities maintain structured, risk-based security programs.

Essential and important entities, as defined by NIS2, include organizations across critical infrastructure and key digital and service sectors throughout the EU. While both groups are subject to the same security and reporting obligations, essential entities face more stringent, ongoing supervision due to their higher systemic importance.

NIS2 Transposition status as of Oct, 2025



The directives operational model is defined in three core provisions. **Article 21** requires organizations to adopt proportionate technical and organizational measures to manage risk. **Article 23** mandates incident reporting within 24 hours of detection followed by a full assessment within 72 hours. **Article 24** establishes the supervisory powers for national authorities to audit, request evidence, and enforce corrective actions.

EU Member States were required to transpose NIS2 by 17 October 2024 however progress varies across the various member states.

The United Kingdom is also introducing a Cyber Security and Resilience Bill that mirrors NIS2 principles by broadening sector scope and tightening reporting requirements to maintain regulatory parity with the EU.

The directive also introduces harmonized penalties. Essential entities can face fines up to €10 million or 2 percent of global turnover, and important entities up to €7 million or 1.4 percent. These sanctions, combined with management accountability requirements, reinforce the expectation that cybersecurity oversight must operate at the executive level.

NIS2 marks a shift from policy to practice. Compliance is no longer a periodic exercise but a living discipline requiring real-time visibility, risk prioritization, and verifiable control.

Note

While Article 23 requires notification "*without undue delay*" and specifies timelines for initial and detailed reports, the exact 24-hour and 72-hour thresholds can be interpreted as aspirational targets rather than absolute hard deadlines. Member states may have slight variations in implementation timelines during national transposition.

Consult with your compliance, regulatory, or legal advisors to confirm national requirements as they may differ between member states.

New Compliance Realities

NIS2 expands the regulatory perimeter significantly. More sectors are now in scope, including public administration (both central, regional and local), space, and critical digital providers. This expansion brings thousands of additional organizations under direct supervision, with management held personally accountable for compliance failures.

The directive also introduces explicit **supply-chain security obligations.** Entities must evaluate and manage risks arising from service providers and vendors, ensuring that third parties apply equivalent security standards. This elevates procurement and vendor due diligence from a contractual formality to a compliance requirement.

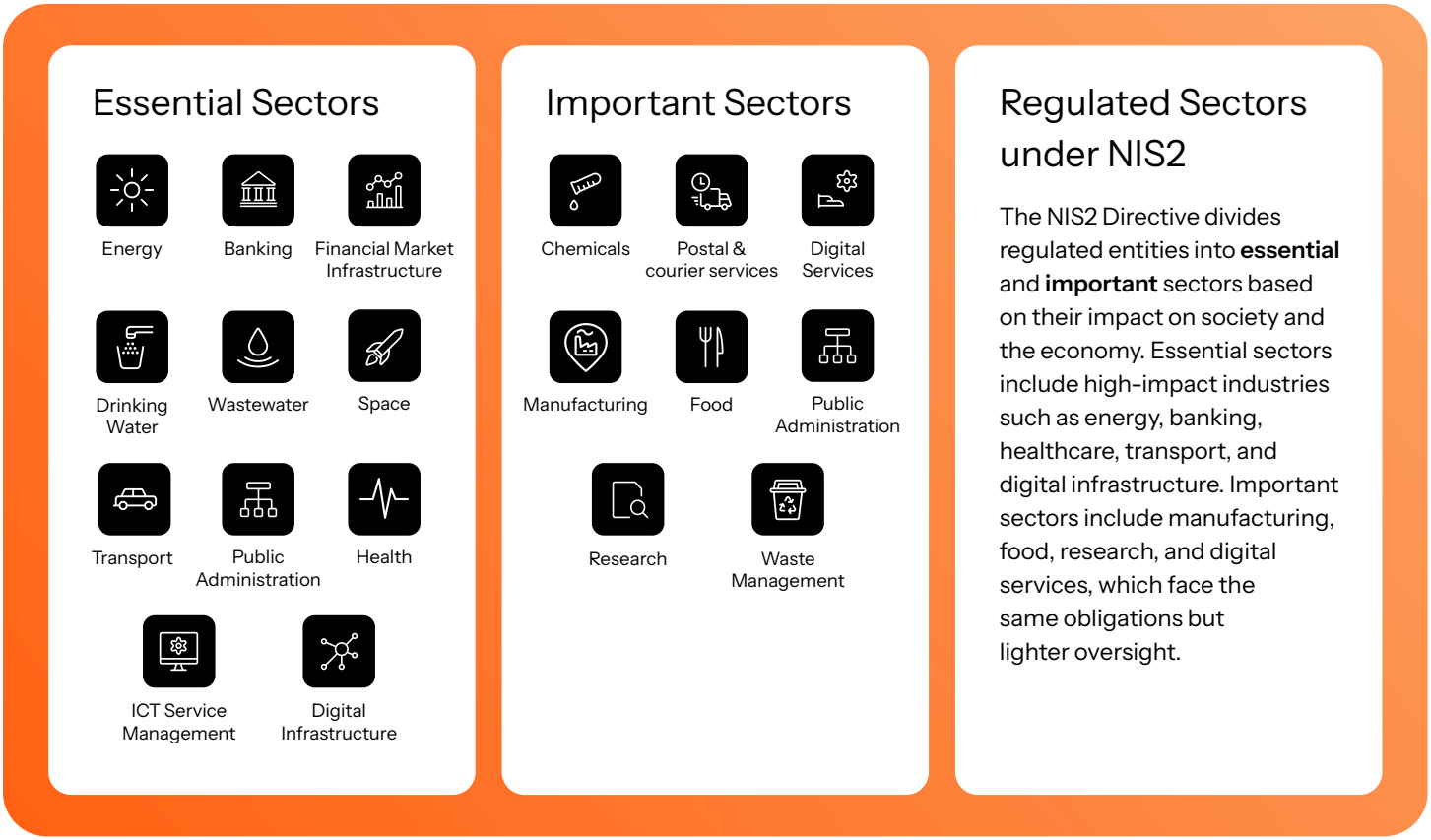
Supervisory authorities are further emphasizing **operational resilience.** Organizations must demonstrate not only that they can prevent and detect incidents, but also that they can recover essential services under disruption. Dependencies on cloud, SaaS, and managed service providers are subject to greater scrutiny, with regulators expecting evidence of resilience testing and contingency planning.

The Emerging Challenge

Meeting NIS2 requirements begins with visibility, yet most organizations still struggle to maintain a unified inventory of assets across IT, OT, cloud, SaaS, and remote environments. Without a single source of truth, entities cannot demonstrate control over the systems and identities in scope.

This challenge is amplified by siloed security tooling. Vulnerability scanners, endpoint agents, cloud dashboards, and identity systems each provide partial views. Gaps emerge in configuration management and risk prioritization, making it difficult to prove compliance with Article 21's demand for proportionate, risk-based measures.

Many organizations still rely on manual audits and spreadsheets to piece together evidence for regulators. This approach cannot keep pace with NIS2's requirement for continuous monitoring, rapid incident reporting, and ongoing supervisory oversight.



Axonius directly addresses these gaps by aggregating, deduplicating and correlating data from more than 1,200 integrations. The platform delivers a consolidated, continuously updated asset inventory and automates evidence collection. This enables compliance teams to replace fragmented, manual processes with a reliable system of record which ensures they can demonstrate resilience, respond faster to incidents, and meet supervisory expectations under NIS2.

From EU directive to Risk Management

Bridging Law and Operations

The NIS2 Directive (Directive (EU) 2022/2555) represents a fundamental shift in how cybersecurity is regulated across the European Union. Where the original NIS Directive focused on establishing baseline security and incident reporting, NIS2 expands the scope and introduces direct accountability for risk management, resilience, and governance.

For affected organizations, compliance is no longer achieved through periodic documentation or certification. It now depends on the ability to demonstrate **ongoing control over risks** that threaten the confidentiality, integrity, and availability of network and information systems. This means that cybersecurity programs must translate legislative obligations into measurable, auditable, and continuously monitored operational practices.

The Concept of Living Compliance

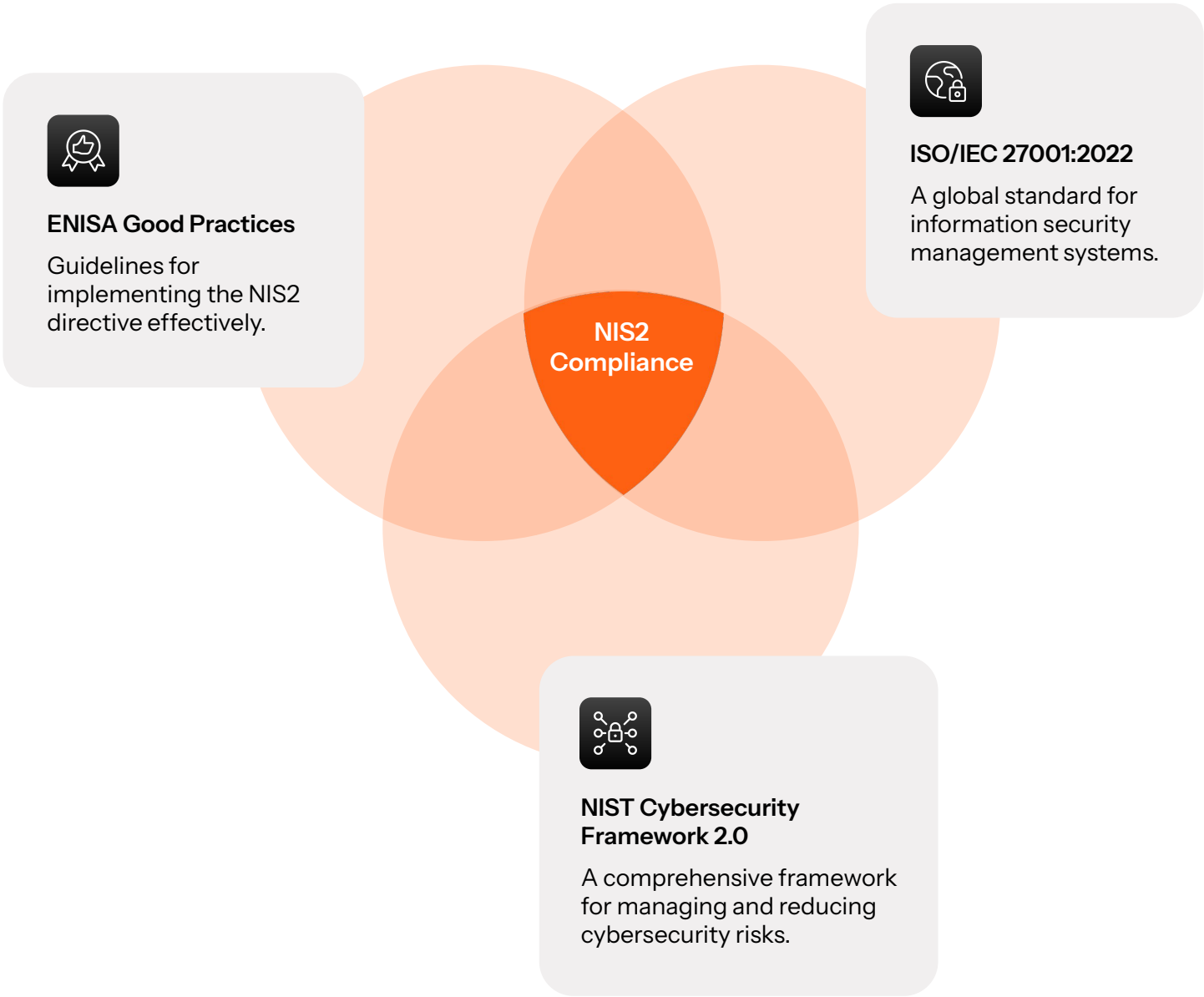
Traditional compliance models have often relied on static assessments, such as annual ISO/IEC 27001 audits or one-off gap analyses against other security frameworks (e.g., CIS Controls v8, NIST CSF). NIS2 challenges that approach Articles 21 and 23 explicitly call for "appropriate and proportionate technical, operational, and organizational measures" that are maintained and adapted to evolving threats. In practical terms, **living compliance** means maintaining a dynamic view of the environment at all times:

- Knowing what assets exist and where they reside
- Detecting configuration drift or unprotected systems as they appear
- Ensuring controls such as access policies, encryption, and patching are continuously enforced
- Recording evidence of these controls for oversight authorities or internal auditors

ENISA's NIS2 guidance reinforces this by promoting continuous monitoring and proactive risk reduction as the foundation of compliance. This shifts the focus from completing audits to maintaining an adaptive security posture that can respond to real-time change.

Framework Alignment

Like most European Union directives, NIS2 isn't prescriptive when it comes to specific technologies or frameworks. Instead, it aligns naturally with internationally recognized standards that define how to operationalize risk management and resilience. Three frameworks stand out for practical implementation:



ISO/IEC 27001:2022

Offers a structured Information Security Management System (ISMS) and control framework aligned to many NIS2 articles. Annex A covers asset management, access control, incident response, and supplier relationships, all directly linked to Articles 21 and 23. The full ISO 27001:2022 standard cannot be legally obtained for free, as it is a copyrighted document sold by ISO and its authorized distributors. Official copies must be purchased directly from the ISO website, national standards bodies, or accredited resellers.

https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

NIST Cybersecurity Framework 2.0 (2024)

introduces a sixth core function, Govern, which strengthens organizational oversight and continuous improvement. Combined with the existing functions — Identify, Protect, Detect, Respond, and Recover. NIST CSF offers a comprehensive structure for aligning cybersecurity operations with NIS2 requirements.

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

ENISA Good Practices for the Implementation of the NIS2 Directive

Acts as a regional interpretation guide that complements ISO and NIST with EU-specific expectations.

https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Rather than inventing new processes, organizations can map and reuse established governance, risk, and compliance processes rather than inventing new ones. This reduces the complexity and cost of implementation whilst ensuring regulatory alignment.

Operational Domains

To effectively transform the directives language into something that is actionable, organizations must operationalize four different control domains that together form the foundation of compliance with NIS2.

Asset Management

Article 21 (2)(a) requires risk management measures based on a complete understanding of the environment. An organization cannot protect what it cannot see. Effective asset management identifies all ICT assets — servers, endpoints, cloud services, network devices, user identities, and dependencies — across business units and subsidiaries. Continuous inventory and classification enable accurate scoping of risk assessments and detection of unauthorized or orphaned assets.

Risk Assessment and Treatment

NIS2 emphasizes a risk-based approach to cybersecurity, requiring organizations to evaluate and prioritize mitigation efforts based on asset criticality, exposure, and potential business impact. Axonius supports this by enabling the development of a risk scoring model that attributes risk to every device or system using context such as ownership, configuration posture, connectivity, and threat exposure. Vulnerability data, where available, further refines this scoring to improve prioritization accuracy. Documented risk treatment plans aligned with these scores demonstrate compliance with Article 21 (2)(b) and (c) while providing measurable, data-driven progress over time.

Incident Handling and Reporting

Under Article 23, entities must detect and report significant incidents within 24 hours of becoming aware of them, followed by a detailed report within 72 hours. Achieving this requires mature detection and response capabilities, automated alerting, and predefined communication channels. Integration with SIEM, SOAR, and ticketing systems ensures that the technical workflow aligns with regulatory deadlines.The context provided by Axonius improves triage efficiency by enabling faster distinction between routine events and reportable incidents. Maintaining an incident register and evidence of response steps is essential for supervisory reviews.

Business Continuity and Supply-Chain Security

Articles 21 (2)(d) and (e) extend risk management to operational continuity and supplier dependencies. Organizations must validate that critical functions can withstand and recover from disruption. This includes documented recovery time objectives, tested backup procedures, and vendor risk assessments. Supply-chain assurance involves verifying that third parties implement equivalent security measures and do not introduce hidden exposures.

Together, these domains establish a continuous control cycle *Visibility* → *Assessment* → *Action* → *Validation.*

The Compliance Control Loop

As with all serious cybersecurity efforts, achieving compliance with NIS2 is not an end state but rather a continuous and ongoing process. Risk evolves, systems change, and new partners enter the supply chain. Organizations therefore need to embed a **compliance control loop** that continually refreshes their understanding of the environment:

Discover all assets and dependencies.

Assess risk and exposure in real time.

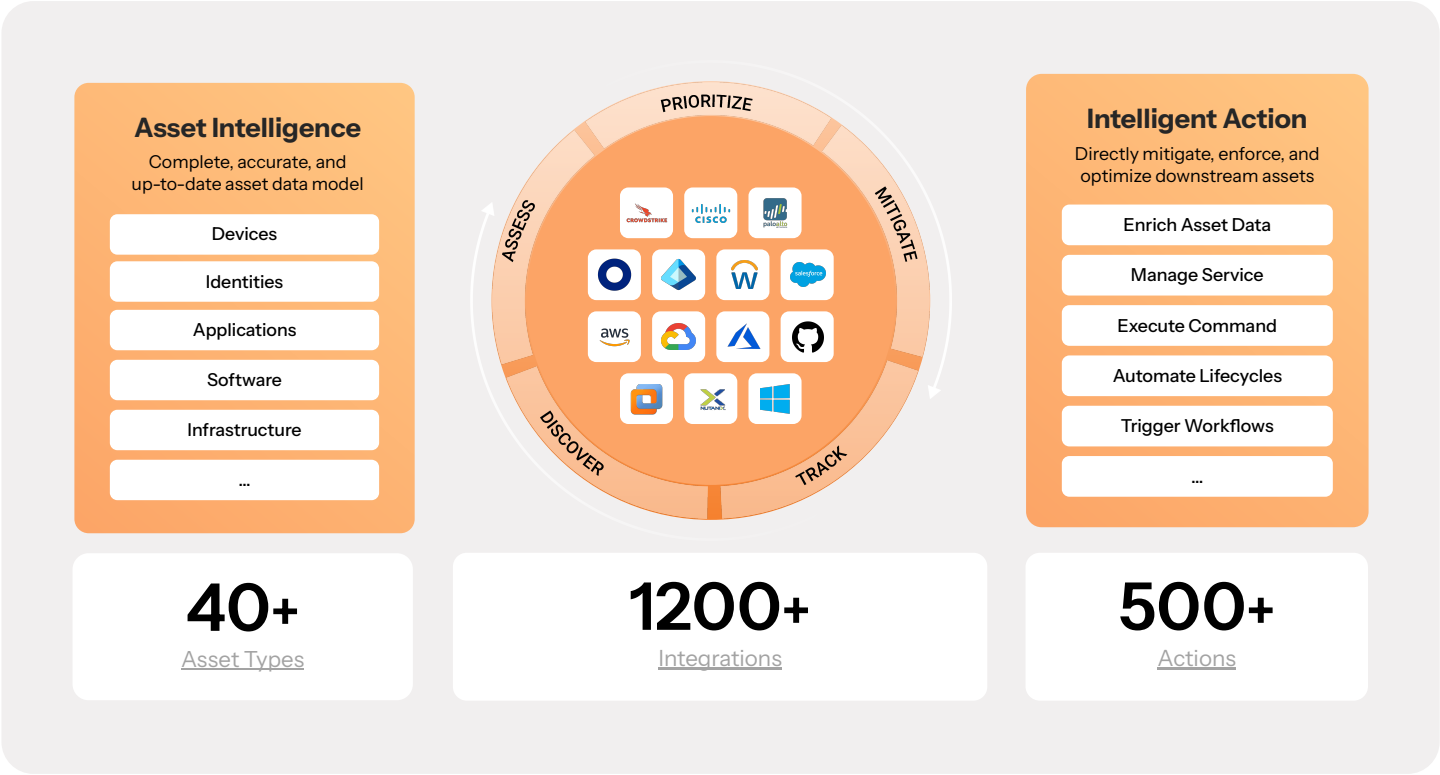
Act through remediation and policy enforcement.

Validate through monitoring and evidence collection.

This cycle reflects the operational intent of NIS2 — to ensure that risk management, incident preparedness, and resilience are demonstrable at any time, not only during audits.

How Axonius Enables NIS2 Compliance

The Axonius Platform at a Glance



Axonius delivers a suite of five core capabilities built on the Axonius Asset Cloud, each addressing the specific needs of security, IT, and operations teams. Every capability leverages the same unified data foundation—providing consistent asset intelligence, bidirectional integrations, and actionable insights tailored to distinct operational challenges.

By establishing a single source of truth for assets, exposures, identities, and software, Axonius enables organizations to apply the Continuous Threat Exposure Management (CTEM) approach consistently across on-premises, private, and public cloud environments.

Axonius Cyber Assets
Ensure every asset across all environments is known, compliant, and protected.

Axonius Software Assets
Gain actionable visibility into software deployment and usage across the enterprise.

Axonius SaaS Management
Inventory the SaaS landscape, mitigate risk, and optimize software spend.

Axonius Exposure Management
Correlate and prioritize exposure data to unify risk findings and drive remediation.

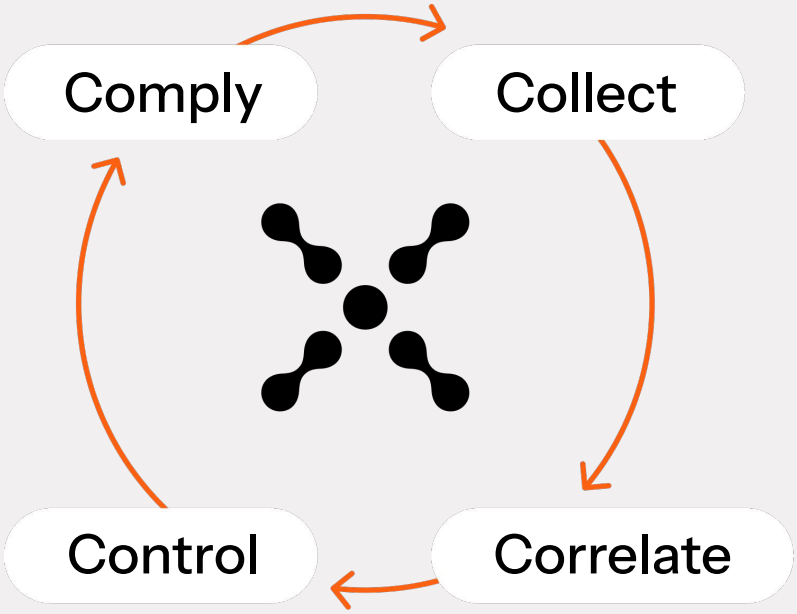
Axonius Identity Management
Consolidate all identity artifacts to transform fragmented user and entitlement data into meaningful security insights.

Capabilities Mapped to NIS2 Articles

NIS2 Requirement	Axonius Capability	Compliance Outcome
Article 21 (2)(a): Risk management and policies	Automated discovery, correlation, and normalization of all assets	Continuous visibility and control
Article 21 (2)(c): Vulnerability handling	Integration with vulnerability scanners (Nessus, Qualys, OpenVAS, Rapid 7 etc) and CMDBs for risk prioritization. Discovery of vulnerabilities outside of vulnerability scanning scope via software versioning and vulnerability enrichments.	Accelerated remediation and audit traceability
Article 21 (2)(e): Supply-chain security	Third-party SaaS inventory and vendor assessment automation	Evidence of due diligence
Article 23: Incident reporting	Integration with SIEM/SOAR tools and alert workflows	Faster detection and 24-hour notification readiness
Article 24: Oversight and accountability	Unified dashboards and compliance metrics	Enables organizations to produce audit-ready evidence and compliance metrics for supervisory authorities, providing executive visibility and traceability to support regulatory oversight.

The Axonius NIS2 Architecture (“Conceptual view”)

At the core of NIS2 readiness is reliable, decision-grade data. The Axonius platform delivers this through the Asset Intelligence Pipeline, a structured architecture that transforms fragmented and often noisy inputs into a unified, actionable model of the entire environment. Each layer plays a specific role in ensuring that the information driving compliance, risk, and remediation is accurate, current, and complete.



1 Step 1: Data Aggregation [Collect]

Axonius continuously collects raw asset, configuration, and identity data from more than 1,200 integrated asset classes, including Active Directory, Okta, EDR/XDR, cloud, and network sources. Its adapter framework handles source-specific logic, authentication, and throttling to retrieve every relevant signal while maintaining reliability and scale. This creates the foundation for a live, continuously updated inventory that goes far beyond the capabilities of CMDBs.

2 Step 2: Correlation and Normalization [Correlate]

The Axonius platform resolves duplicates and conflicting records by correlating entities across systems through field-aware, confidence-weighted logic. Once correlated, all records are normalized into a consistent schema that all asset classes such as devices, identities, software, and policies. This ensures that every query or control is based on a single, trusted source of truth, rather than inconsistent data from siloed tools.

3 Step 3: Policy and Query Engine [CONTROL]

With data unified and normalized, Axonius applies compliance logic directly. The query engine allows organizations to define and enforce rules that map to NIS2 requirements. A typical example could be identifying unmanaged assets, unpatched systems, or accounts missing MFA. These queries form measurable, auditable controls that support Articles 21 and 23 obligations for continuous risk management and incident readiness.

4 Step 4: Automation and Reporting [COMPLY]

Axonius transforms verified data into automated compliance actions. Policy outcomes can trigger remediation workflows, ServiceNow tickets, or reporting processes. Scheduled dashboards and evidence packages align with NIS2's Article 24 oversight needs, ensuring that audit documentation is always available, current, and defensible.

Use Cases in Practice

Visibility and Asset Inventory

NIS2 requires organizations to understand the full scope of their ICT environment. In practice, many enterprises operate across multiple subsidiaries, data centers, and cloud providers, making it difficult to maintain a reliable inventory. Axonius aggregates data from over 1,200 integrations to deliver a continuously updated asset catalog spanning endpoints, servers, cloud workloads, SaaS applications, and user identities. This unified visibility, eliminates blind spots and ensures that compliance teams can demonstrate complete coverage to supervisory authorities.

Exposure Management

Identifying vulnerabilities is only the first step. Regulators expect risk to be prioritized based on the criticality of affected assets. Axonius correlates vulnerability scanner results with asset context such as business function, location, and ownership. This enables organizations to distinguish between low-risk exposures and vulnerabilities that could impact critical services, helping them to meet Article 21 requirements for proportionate risk treatment.

Incident Response Enablement

NIS2 obliges entities to report significant incidents within 24 hours to competent authority, a deadline that cannot be met without rapid detection and triage. By consolidating telemetry from identity systems, endpoints, cloud services, and security controls, Axonius reduces Mean-Time-To-Detect (MTTD) and accelerates incident response workflows. Integration with SIEM and SOAR platforms ensures that alerts are actionable, allowing organizations to respond and report within the mandated timelines.

Audit Readiness

Supervisory authorities are empowered to request evidence of compliance at any time. Producing this evidence manually through spreadsheets and interviews consumes time and resources, and often leaves gaps. Axonius automates evidence collection by maintaining query-based policies that map directly to NIS2 obligations. This allows compliance teams to export audit-ready reports that prove control effectiveness, reducing audit preparation effort and supporting continuous supervision.

Third-Party and Supply Chain Security

Following a surge in third-party and supply chain breaches, NIS2 places strong emphasis on supplier risk management. Under Article 21, organizations must demonstrate their ability to identify and control risks from vendors, service providers, and SaaS platforms. This includes maintaining an up-to-date inventory of assets, managing risks across the supply chain, and ensuring that systems and software—both internal and third-party—remain secure over time. Axonius provides unified visibility into all third-party systems connected to internal networks, exposing unmanaged SaaS, shadow IT, and external dependencies. By monitoring vendor assets alongside internal ones, organizations can validate supplier security, verify contractual compliance, and maintain a consistent risk posture across the entire supply chain.

Partner Ecosystem for NIS2 Readiness

With its centralized data foundation across a wide set of assets, Axonius serves as a compliance enabler. Rather than replacing existing tools, Axonius integrates deeply with security, IT, and operations partners, enhancing the value of each and enabling organizations to meet NIS2 obligations more efficiently and reliably.

Vulnerability Management Integration

Axonius offers adapters for leading vulnerability management platforms such as Tenable, Qualys, Rapid7 and OpenVAS. These integrations allow the platform to aggregate vulnerability data across managed and unmanaged assets, enrich asset context with exposure details, and power risk-based prioritization workflows.

By correlating CVE data with owner, location, role, and criticality, Axonius can help organizations close exposure gaps more strategically. Automated remediation tracking and policy-driven workflows improve the ability to comply with NIS2's risk treatment which obligates a structured risk treatment and continuous monitoring.

IT Service Management and CMDB (ServiceNow)

Through integration with ServiceNow's ITSM and CMDB modules, Axonius enables reconciliation between security and IT operations. Asset and configuration data are validated in real time, reducing discrepancies, enabling audit trails, and supporting evidence collection for regulatory review.

This alignment ensures that security-driven mandates (for patching, configuration changes, or incident workflows) map cleanly into IT process change controls — a necessity under NIS2's operational demands for consistency and accountability.

Identity and Access Management (IAM)

Axonius integrates with IAM and identity providers such as Okta, Microsoft Entra (Azure AD), Ping Identity, and others via adapters. These integrations expose identity metadata (user roles, groups, entitlements, account status) which Axonius correlates with device and system data to detect privilege risks, dormant accounts, orphaned identities, and access anomalies.

This visibility supports NIS2's expectations around access security and helps ensure that identity controls are continuously validated, not only at audit time but dynamically.

Incident Response and Detection

By integrating with platforms such as Splunk, CrowdStrike, and other SIEM/EDR vendors, Axonius injects context into incident workflows. When alerts are raised, Axonius can supply real-time asset, identity, and vulnerability context to responders—reducing mean time to detect and helping meet NIS2's reporting deadlines.

Axonius automates the association of incidents with applicable compliance controls, generating audit-ready evidence for regulators and supporting internal stakeholders in refining incident response plans.

Axonius as the Data Foundation for Compliance Automation

Unified Data Layer
Axonius brings together asset, identity, configuration, and vulnerability data from disparate tools into a single, normalized schema. This unified view becomes the "system of record" for compliance and risk.

Enabler of Automated Compliance Workflows
Because it knows which assets are connected to which tools and their current state, Axonius can help automate compliance workflows: scanning gaps, enforcing configuration rules, tracking remediation work, and collecting evidence.

Audit and Governance Confidence
With query-based controls mapped to NIS2 obligations, Axonius can produce audit-ready reports on demand. This helps reduce the burden on compliance and audit teams, while providing supervisory authorities the transparency they expect.

Interoperability Backbone
Rather than creating replacement tools, Axonius helps existing security and IT tools operate more effectively together. This interoperability makes investment in the broader security stack more durable and aligned to evolving compliance needs.

Flexibility and Future Proofing
The platform's modular adapter architecture and open APIs allow expansion into new domains (e.g., cloud posture, OT, zero-trust segments) as regulators and operational contexts evolve.

Business Impact and ROI

Investing in compliance and security platforms is ultimately a business decision. The Forrester Total Economic Impact™ (TEI) Study of Axonius provides quantifiable evidence of how organizations benefit from greater visibility, automation, and operational efficiency once asset management is unified. The findings demonstrate that improving asset intelligence directly translates into measurable savings and stronger compliance outcomes—both essential under NIS2.

Proven Results from the Forrester TEI Study

Forrester's independent analysis found that organizations deploying Axonius achieved a 156 percent return on investment (ROI) over three years, with a net present value (NPV) of USD 3.22 million and a payback period of less than six months. The total quantified benefit reached USD 5.3 million, against costs of roughly USD 2.1 million over the same period (The Total Economic Impact™ of Axonius, Forrester Consulting, 2023).

156%
is the return on investment (ROI) that organizations achieved over three years, according to Forrester's independent analysis of Axonius deployment.

$3.22M
is the resulting net present value (NPV) calculated in the study.

less than 6 months
was the calculated payback period for the Axonius investment.

$5.3M
was the total quantified benefit reached by the organizations.

$2.1M
was the cost incurred over the same three-year period.

These numbers validate the operational efficiencies Axonius delivers: automation reduces manual tasks, integrations streamline workflows, and a single source of truth enables faster decisions across security and compliance functions.

Streamlined Compliance Operations

Compliance teams using Axonius reported up to 75 percent time savings preparing for risk and compliance reviews and 80 percent less effort compiling audit evidence. By replacing spreadsheets and manual reconciliations with query-based dashboards, organizations eliminate repetitive work and maintain audit readiness at all times.

For entities subject to NIS2, this translates directly into resource optimization. Teams can focus on validating controls and improving resilience instead of gathering data across disconnected systems.

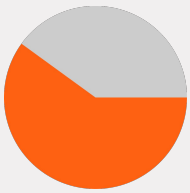
75%
time savings preparing for risk and compliance reviews

80%
less effort compiling audit evidence

Faster Incident Response and Reporting

NIS2 introduces strict reporting obligations and initial notification to competent authority must occur within 24 hours, followed by full reporting within 72 hours. The Forrester TEI study found that organizations reduced incident investigation times by 60 percent after implementing Axonius.

By correlating telemetry from identity, endpoint, and vulnerability systems, Axonius provides context that allows incident responders to pinpoint affected assets immediately. This enables faster containment, clearer communication with authorities, and compliance with NIS2's demanding timelines.



60%
reduced incident investigation times

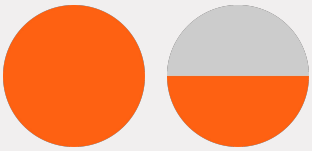
Continuous Measurement of Compliance Performance

The study also showed 90 percent time savings in generating compliance and device-compliance reports. Axonius replaces static snapshots with continuous tracking of internal KPIs—such as "percentage of assets meeting policy requirements" or "mean time to remediate." This supports a data-driven compliance culture and allows executives to monitor risk exposure in real time.

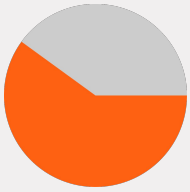
90%
savings in generating compliance and device-compliance reports

Quantified Visibility and Control Gains

Forrester's composite organization discovered 150 percent more assets than previously identified once Axonius was deployed, while reducing the effort needed to maintain accurate inventories by 60 percent. This gain in visibility closes the foundational compliance gap that many organizations face under NIS2 by knowing exactly what assets exist, who owns them, and how they are secured.



150%
more assets than previously identified



60%
less effort needed to maintain accurate inventories

Implementing Axonius for NIS2

1 Step 1: Discovery & Asset Correlation

Connect Axonius to core data sources such as LDAP Directories and Active Directory, cloud platforms, EDR/XDR solutions, and network tools. The platform allows for aggregated and normalized data from all integrated asset classes, creating a unified, continuously updated asset inventory.

2 Step 2: Define Compliance-Based Policies and Queries

Use Axonius' query engine to map technical controls directly to NIS2 obligations. Define policies that identify unmanaged assets, unpatched systems, orphaned accounts, or accounts with missing MFA applied. These queries provide real-time compliance visibility and serve as measurable control evidence for auditors.

3 Step 3: Integrate with Vulnerability Scanners and ITSM

Link Axonius to tools such as Vulnerability Management solutions such as Tenable, Qualys, OpenVAS, Rapid7, and ITSM systems like ServiceNow. This correlation connects risk findings to asset owners and workflows, ensuring vulnerabilities are prioritized, tracked, and remediated in line with NIS2 Article 21 (2)(b) and (2)(c). Integration with ITSM provides audit trails and a structured accountability.

4 Step 4: Automate Remediation and Reporting Workflows

Configure automated actions and scheduled reports that enforce policies, trigger remediation tickets, and export compliance evidence. Dashboards visualize control status, incident metrics, and asset coverage, enabling continuous oversight and readiness for Article 23 reporting or supervisory review.

To ensure continuous governance it is *recommended to use Axonius* powerful dashboard capabilities to set up a set of dashboards where you can easily monitor and follow key telemetry.

Conclusion

NIS2 shifts cybersecurity from periodic certification to continuous, evidence-backed governance where executive leadership is personally held accountable. Performing the obligations under the NIS2 Articles 21, 23, and 24 requires real-time visibility of assets and identities, risk-based prioritization, prepared incident reporting within statutory timelines, and the ability to produce defensible evidence on demand. To achieve this, the operating model is living compliance: discover, assess, act, and validate in a continuous lifecycle.

Axonius provides the practical data foundation for that model. By unifying asset, identity, configuration, and vulnerability data across IT, OT, cloud, and SaaS into a single source of truth, Axonius closes the first and most persistent gap in NIS2 programs: knowing what exists, who owns it, and how it is protected. The platform then links that inventory to operational control, mapping directly to Article 21 risk management measures, enabling Article 23 reporting readiness, and supporting Article 24 oversight through audit-ready reporting. Rather than replacing existing tools, Axonius raises their collective value through correlation, coverage analytics, and automated evidence collection.

The business case is clear. Independent analysis shows a 156% three-year ROI, an NPV of USD 3.22 million, and payback in under six months. Organizations also report up to 75% less time spent on compliance prep, 90% faster reporting, 150% more assets discovered, and 60% gains in both inventory maintenance and incident investigation speed. NIS2 applies a lot of regulatory pressure but it should be seen not as a cost but as an operational advantage.

Effective NIS2 programs share clear indicators of success: complete asset coverage by business unit, declining rates of unmanaged devices, full MFA adoption on critical apps, rapid detection and response times, ownership of critical CVEs, and consistent 24/72-hour reporting readiness.

With the help of Axonious, accountable executives can track progress through dashboards mapped to the relevant articles in the NIS2 directive, while auditors can be served with or receive automated evidence packages generated from saved queries.

NIS2 rewards programs that make visibility and control routine. With Axonius as the unified data layer for assets and identities, compliance becomes a natural output of disciplined operations, while resilience, auditability, and stakeholder trust improve in parallel.

Appendix

A. Compliance Mapping Table (Full Detail)

NIS2 Article	Regulatory requirement	Relevant Axonius capabilities	Compliance outcome	Example Axonius queries/dashboards
21(2)(a)	Risk management based on full asset understanding	Adapter-based discovery across devices, users, cloud, SaaS. Saved Queries and Dashboard panels. Custom discovery cycles.	Unified, continuously updated inventory to scope risk.	Query: Devices missing endpoint agent by vendor. Panel: Asset coverage by BU and source.
21(2)(b)	Identify and analyze cybersecurity risks	Vulnerabilities page and VM adapters for Tenable, Rapid7, Qualys. Risk context by owner, location, business unit.	Ongoing risk assessment and prioritization.	Dashboard: Critical CVEs on Tier-1 assets. Query: CVEs without owner assigned.
21(2)(c)	Vulnerability handling and mitigation	Saved Queries feeding Enforcement to ITSM. ServiceNow CMDB integration and field mapping.	Structured remediation with audit trail and SLA tracking.	Enforcement: Create ServiceNow incident for “Critical CVE and internet exposed.” Panel: TTR by severity.
21(2)(d)	Supply-chain and third-party risk	SaaS Applications discovery and management. Adapter list for vendor systems.	Evidence of supplier due diligence and drift detection.	Query: Unapproved SaaS apps discovered on endpoints. Panel: Third-party assets by vendor risk tier.
21(2)(e)	Business continuity and resilience	Device and service dependency visibility via adapters and queries. Dashboard panels to track backup or redundancy fields when sourced.	Visibility of critical dependencies and resilience gaps.	Panel: Critical services without secondary instance. Query: Servers tagged “critical” missing recent backup flag.

21(2)(f)	Secure acquisition, development, maintenance	Agent coverage and health use cases. Config drift via queryable fields from EDR, cloud, and CMDB.	Patch and hardening posture tracked and provable.	Panel: Patch compliance by environment. Query: Endpoint agents not functioning correctly.
21(2)(g)	Access control and privilege management	IAM and IdP adapters. Users and devices correlation. Saved Queries across users with roles, groups, status.	Least-privilege enforcement and identity hygiene.	Query: Dormant accounts older than 90 days. Panel: Orphaned identities with device access.
21(2)(h)	MFA and secure communications	Query fields from IdP adapters to validate MFA coverage. Dashboards to track MFA adoption per app.	Demonstrable MFA coverage across users and systems.	Query: Users without MFA on business-critical apps. Panel: MFA coverage trend by system.
21(2)(i)	Training and awareness	Dashboards track endpoint control adoption and coverage as proxy KPIs for program effectiveness.	Measurable program participation and device compliance.	Panel: EDR coverage by department. Query: Devices missing security agents.
21(2)(j)	Cryptography and data protection	Ingest encryption or DLP posture attributes from adapters and CMDB where present.	Evidence of encryption and data protection on critical assets.	Panel: Laptops without disk encryption flag. Query: Servers in scope lacking TLS config tag.
21(2)(k)	Incident handling and response	SIEM, SOAR, EDR integrations plus Queries and Dashboards.	Centralized visibility to support coordinated response.	Panel: Assets with no SIEM log source. Query: High-severity EDR alerts with missing ticket link.
23	Incident reporting timelines	Dashboards for MTTD/MTTR. Saved queries feeding “early warning” views.	24-hour early warning readiness and 72-hour report support.	Panel: Open incidents by age. Query: Affected assets list export for regulator notification.
24	Oversight, audit, accountability	Working with dashboard spaces, custom panels, and scheduled reports. Saved Queries as report sources.	On-demand evidence exports and control pass rates.	Dashboard: Article-mapped control status. Scheduled report: Monthly evidence package.

B. Glossary of Terms

AD: Active Directory
API: Application Programming Interface
CAASM: Cyber Asset Attack Surface Management
CMDB: Configuration Management Database
CSF: Cybersecurity Framework
CVE: Common Vulnerabilities and Exposures
EDR: Endpoint Detection and Response
EMEA: Europe, Middle East, and Africa
ENISA: European Union Agency for Cybersecurity
EU: European Union
IAM: Identity and Access Management
ICT: Information and Communications Technology
IEC: International Electrotechnical Commission
ISMS: Information Security Management System
ISO: International Organization for Standardization
IT: Information Technology
KPI: Key Performance Indicator
MFA: Multi-Factor Authentication
MTTD: Mean Time to Detect
MTTR: Mean Time to Respond
NIS2: Network and Information Systems Directive 2
NIST: National Institute of Standards and Technology
NPV: Net Present Value
OT: Operational Technology
ROI: Return on Investment
RTO: Recovery Time Objective
SaaS: Software as a Service
SIEM: Security Information and Event Management
SOAR: Security Orchestration, Automation, and Response
TEI: Total Economic Impact (Forrester study)
USD: United States Dollar
XDR: Extended Detection and Response

C. References

European Union Agency for Cybersecurity. (2025).
Technical implementation guidance on cybersecurity risk management measures (Version 1.0).
https://www.enisa.europa.eu/sites/default/files/2025-06/ENISA_Technical_implementation_guidance_on_cybersecurity_risk_management_measures_version_1.0.pdf

Gartner. (2023). How to manage cybersecurity threats, not episodes. Retrieved from
https://www.gartner.com/en/articles/how-to-manage-cybersecurity-threats-not-episodes

European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

Forrester Consulting. (2023). The Total Economic Impact™ of Axonius.
Forrester Research. https://tei.forrester.com/go/axonius/axonius/?lang=en-us

Axonius. (2025). Axonius product documentation. Retrieved from https://docs.axonius.com/